

AN EXTENSION OF A CONGRUENCE BY KOHNEN

ROMEO MEŠTROVIĆ

ABSTRACT. Let $p > 3$ be a prime, and let $q_p(2) = (2^{p-1} - 1)/p$ be the Fermat quotient of p to base 2. Recently, Z. H. Sun proved that

$$\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv q_p(2) - \frac{p}{2} q_p(2)^2 \pmod{p^2}$$

which is a generalization of a congruence due to W. Kohnen. In this note we give an elementary proof of the above congruence which is based on several combinatorial identities and congruences involving the Fermat quotient $q_p(2)$, harmonic or alternating harmonic sums.

1. INTRODUCTION AND MAIN RESULT

Using a polynomial method, W. Kohnen [12, Theorem] proved that for any odd prime p ,

$$(1) \quad \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv \sum_{k=1}^{(p-1)/2} \frac{(-1)^{k-1}}{k} \pmod{p}.$$

Here, as usually in the sequel, we consider the congruence relation modulo a prime power p^e extended to the ring of rational numbers with denominators not divisible by p . For such fractions we put $m/n \equiv r/s \pmod{p^e}$ if and only if $ms \equiv nr \pmod{p^e}$, and the residue class of m/n is the residue class of mn' where n' is the inverse of n modulo p^e .

In the proof of the above congruence Kohnen [12, the congruence (3) and the congruence after this] showed that

$$(2) \quad \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv -\frac{1}{2} \sum_{k=1}^{p-1} \frac{2^k}{k} \equiv -\frac{1}{2} \sum_{k=1}^{p-1} \frac{(-1)^k}{k} \pmod{p}.$$

2010 *Mathematics Subject Classification*. Primary 11B75, 11A07; Secondary 11B65, 05A10.

Keywords and phrases. congruence, Fermat quotient, harmonic number

Now the congruence (1) immediately follows from (2) and the fact that the sum on the left of (2) can be rewrite as

$$\sum_{k=1}^{(p-1)/2} \frac{(-1)^k}{k} + \sum_{k=1}^{(p-1)/2} \frac{(-1)^{p-k}}{p-k} \equiv 2 \sum_{k=1}^{(p-1)/2} \frac{(-1)^k}{k} \pmod{p}.$$

We point also that Z. W. Sun proved in [23] that for any odd prime p ,

$$(3) \quad \sum_{k=1}^{(p-1)/2} \frac{1}{k \cdot 2^k} \equiv \sum_{k=1}^{\lfloor 3p/4 \rfloor} \frac{(-1)^{k-1}}{k} \pmod{p},$$

where $[a]$ denotes the integer part of a real number a .

The congruence (3) with the bound $\lfloor p/2^n \rfloor$, $n = 1, 2, \dots$, instead of $(p-1)/2$ in the sum on the right hand side of (3) was generalized by W. Kohnen [13, Theorem].

The congruences (1) and (2) may be very interesting if we observe their connection with the Fermat quotient. The Fermat Little Theorem states that if p is a prime and a is an integer not divisible by p , then $a^{p-1} \equiv 1 \pmod{p}$. This gives rise to the definition of the *Fermat quotient of p to base a* ,

$$q_p(a) := \frac{a^{p-1} - 1}{p},$$

which is an integer. It is well known that divisibility of Fermat quotient $q_p(a)$ by p has numerous applications which include the Fermat Last Theorem and squarefreeness testing (see [6], [9] and [19]).

A particular interesting one, due to Glaisher ([7]; also see [10]) for a prime $p \geq 3$, is

$$\sum_{k=1}^{p-1} \frac{2^k}{k} \equiv -2q_p(2) \pmod{p}.$$

Recently, Z. H. Sun [22] established the following extension of the congruence (1).

Theorem. ([22, Theorem 4.1(iii)].) *Let $p \geq 5$ be a prime. Then*

$$(4) \quad \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv q_p(2) - \frac{p}{2} q_p(2)^2 \pmod{p^2}.$$

Sun's proof [22, Lemmas 4.1-4.3] of the congruence (4) is based on the congruential properties of Mirimanoff polynomials obtained by "the anti-derivative method". In his proof it was also used the congruence for the sum $\sum_{k=1}^{(p-1)/2} 1/k \pmod{p^3}$ obtained in [21, Theorem 5.2 (c)] whose proof is deduced by a standard technique for determining power sums $\sum_{k=1}^{(p-1)/2} k^r$ ($r = 1, 2, \dots$) in terms of Bernoulli numbers. Our proof of the Theorem given in the next section is entirely elementary and it is based on some combinatorial identities, numerous classical and new congruences involving the Fermat quotient $q_p(2)$, harmonic and alternating harmonic sums.

These auxiliary congruences are interesting in themselves, such as

$$\sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}}{k} \equiv 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ j \text{ even}}} \frac{1}{ij} \equiv q_p(2)^2 \pmod{p}.$$

Furthermore, notice that Sun's method [23] and Kohnen's method [13] may be applied to extend the congruence (3) modulo p^2 . Both these congruences involve harmonic and alternating harmonic type sums.

Remarks. Quite recently, Z. W. Sun [26, Proof of Theorem 1.1, the congruence after (2.3)] noticed that by a result of Z. H. Sun [22, Corollary 3.3],

$$(5) \quad \sum_{k=1}^{(p-1)/2} \frac{(-1)^{k-1}}{k} \equiv q_p(2) - \frac{p}{2} q_p(2)^2 - (-1)^{(p+1)/2} p E_{p-3} \pmod{p^2},$$

where E_n ($n = 0, 1, 2, \dots$) are *Euler numbers*, that is, integers defined recursively by

$$E_0 = 1, \quad \text{and} \quad \sum_{\substack{0 \leq k \leq n \\ k \text{ even}}} \binom{n}{k} E_{n-k} = 0 \quad \text{for } n = 1, 2, 3, \dots$$

(it is well known that $E_{2n-1} = 0$ for each $n = 1, 2, \dots$).

Comparing (4) and (5), we have

$$\sum_{k=1}^{(p-1)/2} \frac{(-1)^{k-1}}{k} \equiv \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} - (-1)^{(p+1)/2} p E_{p-3} \pmod{p^2},$$

whence we conclude that the congruence (5) can be considered as another generalization of the congruence (1).

Notice that numerous combinatorial congruences recently obtained by Z. W. Sun in [25]–[28] and by Z. H. Sun in [22] contain the Euler numbers E_{p-3} with a prime p . Namely, many of these congruences become "supercongruences" if and only if $E_{p-3} \equiv 0 \pmod{p}$. Using the congruence (5), a computation via *Mathematica 8* shows that only three primes less than $3 \cdot 10^6$ satisfy the condition $E_{p-3} \equiv 0 \pmod{p}$ (such primes are 149, 241 and 2946901). Recall that investigations of such primes have been recently suggested by Z. W. Sun in [26]; namely, in [26, Remark 1.1] Sun found the first and the second such primes, 149 and 241, and used them to discover curious supercongruences (1.2)–(1.5) from Theorem 1.1 in [26] involving E_{p-3} .

By statistical considerations (cf. [4, p. 447] and [16] in relation to search for Wieferich and Fibonacci-Wieferich and Wolstenholme primes, respectively), in an interval $[x, y]$, there are expected to be

$$\sum_{x \leq p \leq y} \frac{1}{p} \approx \log \frac{\log y}{\log x}$$

primes satisfying $E_{p-3} \equiv 0 \pmod{p}$. In particular, it follows that in the interval $[3 \cdot 10^6, 10^{18}]$ we can expect about 1.0221 such primes. Also notice

that in accordance to the above estimation, in the interval $[2, 3 \cdot 10^6]$ we can expect about 3.06882 primes p such that $E_{p-3} \equiv 0 \pmod{p}$; as noticed previously, our computation shows that all these primes are 149, 241 and 2946901.

Recall that a prime p is said to be a *Wolstenholme prime* if it satisfies the congruence

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4},$$

or equivalently (cf. [15, Corollary on page 386]; also see [7]) that p divides the numerator of B_{p-3} . The only two known such primes are 16843 and 2124679, and by a recent result of McIntosh and Roettger from [16, pp. 2092–2093], these primes are the only two Wolstenholme primes less than 10^9 . Nevertheless, by using an argument based on the prime number theorem, McIntosh [15, page 387] conjectured that there are infinitely many Wolstenholme primes. Since in accordance to the our investigations of $E_{p-3} \equiv 0 \pmod{p}$ up to $p < 3 \cdot 10^6$, we can assume that the remainder modulo p of E_{p-3} is random. Then applying the previous mentioned McIntosh's argument we propose the following

Conjecture. There are infinitely many primes p such that $E_{p-3} \equiv 0 \pmod{p}$.

2. PROOF OF THE THEOREM

For a nonnegative integer n let

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

be the n th *harmonic number* (we assume that $H_0 = 0$).

We begin with well known result.

Lemma 2.1. ([29, Lemma 2.1]). *If p is an odd prime, then*

$$(6) \quad \binom{p-1}{k} \equiv (-1)^k - (-1)^k p H_k + (-1)^k p^2 \sum_{1 \leq i < j \leq k} \frac{1}{ij} \pmod{p^3}$$

for each $k = 1, 2, \dots, p-1$.

Proof. For a fixed $1 \leq k \leq p-1$ we have

$$\begin{aligned} (-1)^k \binom{p-1}{k} &= \prod_{i=1}^k \left(1 - \frac{p}{i}\right) \equiv 1 - \sum_{i=1}^k \frac{p}{i} + \sum_{1 \leq i < j \leq k} \frac{p^2}{ij} \pmod{p^3} \\ &= 1 - p H_k + p^2 \sum_{1 \leq i < j \leq k} \frac{1}{ij} \pmod{p^3}, \end{aligned}$$

which is actually the congruence (6). □

The following congruences are well known (e.g., see [24, Proof of Corollary 1.2]).

Lemma 2.2. *Let $p \geq 5$ be a prime. Then*

$$\begin{aligned}
 (7) \quad q_p(2) &\equiv \frac{1}{2} \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \equiv - \sum_{\substack{1 \leq i \leq p-1 \\ i \text{ even}}} \frac{1}{i} = -\frac{1}{2} H_{(p-1)/2} \\
 &\equiv \sum_{\substack{1 \leq i \leq p-1 \\ i \text{ odd}}} \frac{1}{i} \pmod{p}.
 \end{aligned}$$

Proof. Applying the binomial formula, using the identity $\frac{1}{n} \binom{n}{k} = \frac{1}{k} \binom{n-1}{k-1}$ and the congruence (6) reduced modulo p , we find that

$$\begin{aligned}
 (8) \quad 2q_p(2) &= \frac{2^p - 2}{p} = \frac{(1+1)^p - 2}{p} = \frac{\sum_{k=1}^{p-1} \binom{p}{k}}{p} \\
 &= \sum_{k=1}^{p-1} \frac{1}{k} \binom{p-1}{k-1} \equiv \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \pmod{p}.
 \end{aligned}$$

By *Wolstenholme's theorem* ([30]; also see [1, Theorem 1] or [11]), if p is a prime greater than 3, then the numerator of the fraction

$$H_{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p^2 . This together with the congruence (8) gives

$$\begin{aligned}
 2q_p(2) &\equiv \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} = \sum_{k=1}^{p-1} \frac{1}{k} - 2 \sum_{\substack{1 \leq i \leq p-1 \\ i \text{ even}}} \frac{1}{i} \\
 &\equiv -2 \sum_{\substack{1 \leq i \leq p-1 \\ i \text{ even}}} \frac{1}{i} = -H_{(p-1)/2} \pmod{p}.
 \end{aligned}$$

Analogously, we obtain the third congruence from (7). \square

Lemma 2.3. *Let $p \geq 5$ be a prime. Then*

$$(9) \quad \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}$$

and

$$(10) \quad \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} \equiv 0 \pmod{p}.$$

Proof. By a result of Bayat [2, Theorem 3 (ii)], for any prime $p \geq 5$ the numerator of the fraction $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$ is divisible by p , which is the congruence (9).

Notice that the set of all quadratic residues modulo p is actually the set $\{1^2, 2^2, \dots, ((p-1)/2)^2\}$. Since $i^2 \equiv (p-i)^2 \pmod{p}$ for each $i = 1, \dots, (p-1)/2$, it follows that regarding modulo p this set coincides with

the set $\{((p+1)/2)^2, ((p+3)/2)^2, \dots, (p-1)^2\}$, and so by the mentioned result of Bayat, we have

$$\sum_{k=1}^{(p-1)/2} \frac{1}{k^2} \equiv \frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}.$$

This is (10) and the proof is completed. \square

Lemma 2.4. *Let n be a positive integer. Then*

$$(11) \quad \sum_{k=1}^{2n} (-1)^k H_k = \frac{1}{2} H_n,$$

$$(12) \quad \sum_{k=2}^{2n} \sum_{1 \leq i < j \leq k} \frac{(-1)^k}{ij} = \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ even}}} \frac{1}{ij}$$

and

$$(13) \quad \sum_{k=2}^{2n} \frac{(-1)^k H_{k-1}}{k} = 2 \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ even}}} \frac{1}{ij} - \sum_{1 \leq i < j \leq 2n} \frac{1}{ij}.$$

Proof. The identity (11) easily follows by induction on n , and hence its proof may be omitted.

In order to prove the equality (12), observe that for fixed i, j with $1 < j \leq 2n$ the sum of all terms on the left of (12) containing $1/(ij)$ is equal to

$$\frac{1}{ij} \sum_{k=j}^{2n} (-1)^k = \begin{cases} 0 & \text{if } j \text{ is odd} \\ 1 & \text{if } j \text{ is even.} \end{cases}$$

This immediately yields (12).

The equality in (13) is satisfied as follows.

$$\begin{aligned} \sum_{k=1}^{2n} \frac{(-1)^k H_{k-1}}{k} &= \sum_{k=2}^{2n} \frac{(-1)^k}{k} \sum_{i=1}^{k-1} \frac{1}{i} = \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ even}}} \frac{1}{ij} - \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ odd}}} \frac{1}{ij} \\ &= \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ even}}} \frac{1}{ij} - \left(\sum_{1 \leq i < j \leq 2n} \frac{1}{ij} - \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ even}}} \frac{1}{ij} \right) \\ &= 2 \sum_{\substack{1 \leq i < j \leq 2n \\ j \text{ even}}} \frac{1}{ij} - \sum_{1 \leq i < j \leq 2n} \frac{1}{ij}. \end{aligned}$$

This completes the proof. \square

Lemma 2.5. *Let $p \geq 5$ be a prime. Then*

$$(14) \quad q_p(2)^2 \equiv 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ even}, j \text{ even}}} \frac{1}{ij} \equiv 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ odd}}} \frac{1}{ij} \pmod{p}.$$

Proof. The second congruence in (7) from Lemma 2.2 and the congruence (10) from Lemma 2.3 immediately give

$$\begin{aligned} q_p(2)^2 &\equiv \left(\sum_{\substack{1 \leq i \leq p-1 \\ i \text{ even}}} \frac{1}{i} \right)^2 = 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ even}, j \text{ even}}} \frac{1}{ij} + \sum_{\substack{1 \leq i \leq p-1 \\ i \text{ even}}} \frac{1}{i^2} \pmod{p} \\ &= 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ even}, j \text{ even}}} \frac{1}{ij} + \frac{1}{4} \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} \equiv 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ even}, j \text{ even}}} \frac{1}{ij} \pmod{p}. \end{aligned}$$

Further, we have

$$\sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ even}, j \text{ even}}} \frac{1}{ij} = \sum_{\substack{1 \leq j < i \leq p-1 \\ j \text{ odd}, i \text{ odd}}} \frac{1}{(p-i)(p-j)} \equiv \sum_{\substack{1 \leq j < i \leq p-1 \\ j \text{ odd}, i \text{ odd}}} \frac{1}{ij} \pmod{p}.$$

The above two congruences yield (14). \square

Lemma 2.6. *Let $p \geq 5$ be a prime. Then*

$$(15) \quad \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}}{k} \equiv 2 \sum_{\substack{1 \leq i < j \leq p-1 \\ j \text{ even}}} \frac{1}{ij} \equiv q_p(2)^2 \pmod{p}.$$

Proof. Applying the fact that $p \mid H_{p-1}$ and the congruence (9) of Lemma 2.3 to the left hand side of the identity

$$2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} = \left(\sum_{k=1}^{p-1} \frac{1}{k} \right)^2 - \sum_{k=1}^{p-1} \frac{1}{k^2},$$

we immediately obtain

$$(16) \quad \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} \equiv 0 \pmod{p}.$$

Substituting the congruence (16) into the identity (13) of Lemma 2.4 with $2n = p - 1$, we obtain the first congruence from (15).

Further, taking the first congruence of (14) from Lemma 2.5, we obtain

$$\begin{aligned} (17) \quad \sum_{\substack{1 \leq i < j \leq p-1 \\ j \text{ even}}} \frac{1}{ij} &= \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ even}, j \text{ even}}} \frac{1}{ij} + \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \\ &\equiv q_p(2)^2 + \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \pmod{p}. \end{aligned}$$

Hence, it remains to determine $S := \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij}$ modulo p . Let

$$A := \{(i, j) : 1 \leq i < j \leq p-1, i \text{ odd}, j \text{ even}\}.$$

Then it is easily seen that the map $f : A \rightarrow \mathbb{N}^2$ defined as $f(i, j) = (j - i, j)$ is a bijection from A to A , and thus

$$(18) \quad \begin{aligned} 2S &= \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \left(\frac{1}{ij} + \frac{1}{(j-i)j} \right) = \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \frac{1}{i(j-i)} \\ &\equiv - \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \frac{1}{i(p - (j-i))} := -S' \pmod{p}. \end{aligned}$$

Observing also that the map $g : A \rightarrow \mathbb{N}^2$ defined as $g(i, j) = (i, p - (j - i))$ is also a bijection from A to A , it follows that $S' = S$. Replacing this equality into (18), we obtain $3S \equiv 0 \pmod{p}$, that is,

$$S = \sum_{\substack{1 \leq i < j \leq p-1 \\ i \text{ odd}, j \text{ even}}} \frac{1}{ij} \equiv 0 \pmod{p}.$$

Substituting this into (17), we obtain the second congruence of (15). This completes the proof. \square

Lemma 2.7. *Let $p \geq 5$ be a prime. Then*

$$(19) \quad H_{(p-1)/2} \equiv -2q_p(2) + pq_p(2)^2 \pmod{p^2}.$$

Proof. After summation of the congruence (6) of Lemma 2.1 over k , using the identities (11) and (12) from Lemma 2.4 with $n = (p-1)/2$, we find that

$$\begin{aligned} 2^{p-1} - 1 &= (1+1)^{p-1} - 1 = \sum_{k=1}^{p-1} \binom{p-1}{k} \\ &\equiv \sum_{k=1}^{p-1} (-1)^k - p \sum_{k=1}^{p-1} (-1)^k H_k + p^2 \sum_{k=1}^{p-1} \sum_{1 \leq i < j \leq k} \frac{(-1)^k}{ij} \pmod{p^3} \\ &= -\frac{p}{2} H_{(p-1)/2} + p^2 \sum_{\substack{1 \leq i < j \leq p-1 \\ j \text{ even}}} \frac{1}{ij} \pmod{p^3}. \end{aligned}$$

Dividing the above congruence by p , we immediately obtain

$$q_p(2) \equiv -\frac{1}{2} H_{(p-1)/2} + p \sum_{\substack{1 \leq i < j \leq p-1 \\ j \text{ even}}} \frac{1}{ij} \pmod{p^2},$$

whence substituting the second congruence in (15) from Lemma 2.6, we immediately obtain (19). \square

Remarks. The congruence (19) was proved in 1938 by E. Lehmer [14, the congruence (45), p. 358]. This proof followed the method of Glaisher [8], which depends on Bernoulli polynomials of fractional arguments. Using (19) and other similar congruences, E. Lehmer obtained various criteria for the first case of Fermat Last Theorem (cf. [19]). In the conclusion of this paper [14, p. 360] it was observed that a beautiful Morley's congruence

[17] published in 1895, follows immediately inserting the congruences (19) and (10) of Lemma 2.3 into (6) of Lemma 2.1 with $k = (p-1)/2$. This congruence asserts that for a prime $p > 3$,

$$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} 4^{p-1} \pmod{p^3}.$$

Notice also that the congruence (19) reduced modulo p asserts that $H_{(p-1)/2} \equiv -2q_p(2) \pmod{p}$, which is the congruence established in 1850 by Eisenstein [5]. On the other hand, in 2002 T. Cai [3, Theorem 1] generalized the congruence (19) to a congruence modulo a square of an arbitrary positive integer.

Lemma 2.8. *Let $p \geq 5$ be a prime. Then*

$$(20) \quad \sum_{k=1}^{p-1} (-1)^k H_k^2 \equiv q_p(2)^2 \pmod{p^2}$$

and

$$(21) \quad \sum_{k=1}^{p-1} \binom{p-1}{k} H_k \equiv -q_p(2) - \frac{1}{2} p q_p(2)^2 \pmod{p^2}.$$

Proof. The identity $H_k = H_{k-1} + 1/k$ gives

$$\begin{aligned} \sum_{k=1}^{p-1} (-1)^k H_k^2 &= \sum_{k=1}^{p-1} (-1)^k \left(H_{k-1} + \frac{1}{k} \right)^2 \\ &= \sum_{k=1}^{p-1} (-1)^k H_{k-1}^2 + 2 \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}}{k} + \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} \\ &= - \sum_{k=1}^{p-1} (-1)^k H_k^2 + H_{p-1}^2 + 2 \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}}{k} + \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2}, \end{aligned}$$

whence

$$(22) \quad 2 \sum_{k=1}^{p-1} (-1)^k H_k^2 = H_{p-1}^2 + 2 \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}}{k} + \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2}.$$

Since

$$\sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} = 2 \sum_{\substack{1 \leq k \leq p-1 \\ k \text{ even}}} \frac{1}{k^2} - \sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{1}{2} \sum_{k=1}^{(p-1)/2} \frac{1}{k^2} - \sum_{k=1}^{p-1} \frac{1}{k^2},$$

taking into this (9) and (10) of Lemma 2.3, it follows that

$$(23) \quad \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} \equiv 0 \pmod{p}.$$

Substituting the congruences $H_{p-1} \equiv 0 \pmod{p}$, (15) from Lemma 2.6 and (23) into (22), we find that

$$2 \sum_{k=1}^{p-1} (-1)^k H_k^2 = H_{p-1}^2 + 2 \sum_{k=1}^{p-1} \frac{(-1)^k H_{k-1}}{k} + \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} \equiv 2q_p(2)^2 \pmod{p}.$$

This proves the congruence (20).

The congruence (6) from Lemma 2.1 reduced modulo p^2 , the identity (11) of Lemma 2.4, the congruences (20) and (19) of Lemma 2.7 yield

$$\begin{aligned} \sum_{k=1}^{p-1} \binom{p-1}{k} H_k &\equiv \sum_{k=1}^{p-1} (-1)^k H_k - p \sum_{k=1}^{p-1} (-1)^k H_k^2 \pmod{p^2} \\ (24) \quad &= \frac{1}{2} H_{(p-1)/2} - p \sum_{k=1}^{p-1} (-1)^k H_k^2 \\ &\equiv \frac{1}{2} (-2q_p(2) + pq_p(2)^2) - pq_p(2)^2 \pmod{p^2} \\ &= -q_p(2) - \frac{1}{2} pq_p(2)^2 \pmod{p^2}. \end{aligned}$$

This is the congruence (21) and the proof is completed. \square

Finally, in order to prove Theorem, we still need the following identity established in [18, Eq. (40)] by using the *Sigma* package.

Lemma 2.9. *For a positive integer n we have*

$$(25) \quad \sum_{k=1}^n \binom{n}{k} H_k = 2^n H_n - 2^n \sum_{k=1}^n \frac{1}{k \cdot 2^k}.$$

Proof. We proceed by induction on $n \geq 1$. As (25) is trivially satisfied for $n = 1$, we suppose that this is also true for some $n \geq 1$. Then using the induction hypothesis (in the last equality below), the identities $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ and $H_k = H_{k-1} + 1/k$ with $1 \leq k \leq n+1$, we get

$$\begin{aligned} \sum_{k=1}^{n+1} \binom{n+1}{k} H_k &= \sum_{k=1}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k} \right) H_k \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} \left(H_{k-1} + \frac{1}{k} \right) + \sum_{k=1}^{n+1} \binom{n}{k} H_k \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} H_{k-1} + \sum_{k=1}^{n+1} \frac{1}{k} \binom{n}{k-1} + \sum_{k=1}^n \binom{n}{k} H_k \\ &= 2 \sum_{k=1}^n \binom{n}{k} H_k + \sum_{k=1}^{n+1} \frac{1}{k} \binom{n}{k-1} \\ &= 2^{n+1} H_n - 2^{n+1} \sum_{k=1}^n \frac{1}{k \cdot 2^k} + \sum_{k=0}^n \frac{1}{k+1} \binom{n}{k}. \end{aligned}$$

Hence, the induction proof will be finished if we prove that

$$2^{n+1}H_n - 2^{n+1} \sum_{k=1}^n \frac{1}{k \cdot 2^k} + \sum_{k=0}^n \frac{1}{k+1} \binom{n}{k} = 2^{n+1}H_{n+1} - 2^{n+1} \sum_{k=1}^{n+1} \frac{1}{k \cdot 2^k}.$$

Substituting $H_{n+1} = H_n + 1/(n+1)$ into above relation, it immediately reduces to

$$\sum_{k=0}^n \frac{1}{k+1} \binom{n}{k} = 2^{n+1} \left(\frac{1}{n+1} - \frac{1}{(n+1)2^{n+1}} \right) = \frac{2^{n+1} - 1}{n+1}.$$

The above equality is well known identity (see e.g., [20, Identity 13, p. 3135]) of Lemma 2.2, and it can be derived by using the binomial formula and the identity $\frac{1}{n+1} \binom{n+1}{k} = \frac{1}{k} \binom{n}{k-1}$ with $1 \leq k \leq n+1$ as follows.

$$\frac{2^{n+1} - 1}{n+1} = \frac{1}{n+1} \sum_{k=1}^{n+1} \binom{n+1}{k} = \sum_{k=1}^{n+1} \frac{1}{k} \binom{n}{k-1} = \sum_{k=0}^n \frac{1}{k+1} \binom{n}{k}.$$

Thus, the induction proof is completed. \square

Proof of the Theorem. The identity (25) from Lemma 2.9 with $n = p-1$ becomes

$$2^{p-1}H_{p-1} - 2^{p-1} \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} = \sum_{k=1}^{p-1} \binom{p-1}{k} H_k.$$

Substituting the Wolstenholme's congruence $H_{p-1} \equiv 0 \pmod{p^2}$ and the congruence (21) of Lemma 2.8 into above identity, we find that

$$-2^{p-1} \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv -q_p(2) - \frac{1}{2}pq_p(2)^2 \pmod{p^2},$$

whence we obtain

$$\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv \frac{q_p(2) + \frac{1}{2}pq_p(2)^2}{2^{p-1}} = \frac{q_p(2) + \frac{1}{2}pq_p(2)^2}{1 + pq_p(2)} \pmod{p^2},$$

which in view of the fact that $1/(1 + pq_p(2)) \equiv 1 - pq_p(2) \pmod{p^2}$, gives

$$\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv \left(q_p(2) + \frac{1}{2}pq_p(2)^2 \right) (1 - pq_p(2)) \equiv q_p(2) - \frac{p}{2}q_p(2)^2 \pmod{p^2}.$$

This is the desired congruence (4). \square

REFERENCES

- [1] E. Alkan, Variations on Wolstenholme's theorem, *Amer. Math. Monthly* **101** (1994), 1001-1004.
- [2] M. Bayat, A generalization of Wolstenholme's Theorem, *Amer. Math. Monthly* **104** (1997), 557-560.
- [3] T. Cai, A congruence involving the quotients of Euler and its applications (I), *Acta Arithmetica* **103** (2002), 313-320.

- [4] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 443–449.
- [5] G. Eisenstein, Eine neue Gattung zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden, *Bericht. K. Pruss. Akad. Wiss.* 1850, 36–42; see also G. Eisenstein, *Mathematische Werke*, Vol. II, Chelsea, 1975, 705–711.
- [6] R. Ernvall and T. Metsänkylä, On the p -divisibility of Fermat quotients, *Math. Comp.* **66** (1997), 1353–1365.
- [7] J. W. L. Glaisher, On the residues of the sums of products of the first $p - 1$ numbers, and their powers, to modulus p^2 or p^3 , *Q. J. Math.* **31** (1900), 321–353.
- [8] J. W. L. Glaisher, On the residues of the sums of the inverse powers of numbers in arithmetical progression, *Q. J. Math.* **32** (1901), 271–305.
- [9] A. Granville, *Some conjectures related to Fermat's Last Theorem*, Number Theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, 177–192.
- [10] A. Granville, The square of the Fermat quotient, *Integers*, **4** (2004), # A22.
- [11] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic Mathematics–Burnaby, BC 1995*, CMS Conf. Proc., vol. 20, American Mathematical Society, Providence, RI, 1997, 253–276.
- [12] W. Kohnen, A simple congruence modulo p , *Amer. Math. Monthly* **104** (1997), 444–445.
- [13] W. Kohnen, Some congruences modulo primes, *Monatsh. Math.* **127** (1999), 321–324.
- [14] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Ann. Math.* **39** (1938), 350–360.
- [15] R. J. McIntosh, On the converse of Wolstenholme's theorem, *Acta Arith.* **71** (1995), 381–389.
- [16] R. J. McIntosh and E. L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, *Math. Comp.* **76** (2007), 2087–2094.
- [17] F. Morley, Note on the congruence $2^{4n} \equiv (-1)^n(2n)!/(n!)^2$, where $2n+1$ is a prime, *Ann. Math.* **9** (1895), 168–170.
- [18] P. Paule and C. Schneider, Computer proofs of a new family of harmonic number identities, *Adv. in Appl. Math.* **31** (2003), 359–378.
- [19] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, Heidelberg, Berlin, 1979.
- [20] M. Z. Spivey, Combinatorial sums and finite differences, *Discrete Math.* **307** (2007), 3130–3146.
- [21] Z. H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, *Discrete Appl. Math.* **105** (2000), 193–223.
- [22] Z. H. Sun, Congruences involving Bernoulli and Euler numbers, *J. Number Theory*, **128** (2008), 280–312.
- [23] Z. W. Sun, A congruence for primes, *Proc. Amer. Math. Soc.* **123** (1995), 1341–1346.
- [24] Z. W. Sun, Binomial coefficients, Catalan numbers and Lucas quotients, *Sci. China Math.* **53** (2010), 2473–2488; preprint arXiv:0909.5648v11 [math.NT] (2010).
- [25] Z. W. Sun, On Delannoy numbers and Schröder numbers, *J. Number Theory* **131** (2011), 2387–2397; preprint arXiv:1009.2486v4 [math.NT] (2011).
- [26] Z. W. Sun, Super congruences and Euler numbers, *Sci. China Math.* **54** (2011), article in press, preprint arXiv:1001.4453v19 [math.NT] (2011).
- [27] Z. W. Sun, A refinement of the Hamme–Mortenson congruence, preprint arXiv:1011.1902v5 [math.NT] (2011).
- [28] Z. W. Sun, On congruences related to central binomial coefficients, *J. Number Theory* **131** (2011), 2219–2238; preprint arXiv:0911.2415v16 [math.NT] (2011).

- [29] Z. W. Sun, Arithmetic theory of harmonic numbers, *Proc. Amer. Math. Soc.*, article in press, S 0002-9939(2011)10925-0; preprint `arXiv:0911.4433v6 [math.NT]` (2009).
- [30] J. Wolstenholme, On certain properties of prime numbers, *Quart. J. Pure Appl. Math.* **5** (1862), 35–39.

DEPARTMENT OF MATHEMATICS, MARITIME FACULTY, UNIVERSITY OF MONTENEGRO, DOBROTA 36, 85330 KOTOR, MONTENEGRO `ROMEO@AC.ME`